KTH Computer Science
and Communication

Proof of Work

A load measure approach to cryptographic mitigation of denial-of-service attacks

FREDRIK LILKAER, CHRISTOPHER TELJSTEDT

Bachelor's Thesis
Supervisor: Douglas Wikström

1 Introduction

The Internet continues to grow and has since a time back fulfilled it's early promise to enable a single source to be connected to several millions of geographically dispersed computers. However, as a consequence it has introduced security flaws of a new magnitude, allowing a single computer to potentially be attacked from millions of sources at once.

Denial of Service continues to plague internet services even if they are efficaciously protected against intrusive security breaches, as evidenced by the recent attack on Spamhaus [1]. A denial of service attack is essentially a targeted effort to prevent a service from servicing legitimate requests by draining the underlying computer resources. Such an attack is executed by having each attacking machine performing only small load of the total work, relying on the cumulative work to overload the target system.

In this paper, we focus on the computational approach to combatting denial of service attacks and to improve service survivability. This concept was originally proposed by Dwork and Naor in their report "Pricing via Processing or Combatting Junk Mail" and then the idea was further researched in "On Memory-Bound Functions for Fighting Spam". The "proof of work" is cryptographic in flavor and the idea is essentially to respond with a problem that is moderately hard to compute but easy to verify. Dwork and Naor originally called this a *pricing function* because of it's economic origin. They introduced this concept as a way to fight e-mail spam by increasing the costs of sending spam, thus making e-mail spam economically unfeasible.

In recent studies researchers have shown an increased interest in the Proof of Work (PoW) concept in order to prevent or mitigate the effects of a DoS attacks instead of fighting spam.

1.1 Background

1.2 Problem definition

Proof of Work has been shown to potentially work as a prevention mechanism to at least mitigate the effects of a DoS attack without making an as assumption about the source.[källa] However, Laurie and Clayton concluded in the paper *"Proof of Work" proves not to work*, that PoW on it's own, is not a feasible solution to fighting spam and denial of service attacks. This is because the classical implementation of Proof of Work does not seperate legitimate users from attackers. Hence, problems from a Proof of Work protected system would not discourage abusers of the system without having an unacceptable effect on legitimate users.

1.3 Problem statement

With the problem defined the question at hand is thus if it is possible to develop a Proof of Work protocol that is independent of client characteristics.

- Is there a viable way to implement a Proof of Work system so that the system's resources are accessable by a diverse variety of devices?

- How should the protocol be optimised for low impact on legitimate client behaviour and high impact on malicious behaviour?

- What advantages and disadvantages does proof of work concept bring in practice and in which applications could it be an improvement to current security?

2 Purpose and method

The purpose of this study is to research ways to improve the classical Proof of Work in such a way that legitimate users are less affected by the Proof of Work than the participants of a DoS attack. Furthermore find a way to dynamically scale the required proof of work when dealing with different hardware.

2.1 Scope and delimitations

Scope:
The coverage of this study .....
The study consists of .....
The study covers the .....
This study is focus on .....

Delimitations:
The study does not cover the .....
The researcher limited this research to .....
This study is limited to .....

Bibliography

[1] BBC News Dave Lee Technology reporter. *Global internet slows after 'biggest attack in history'*. 2013. URL: http://www.bbc.co.uk/news/technology-21954636 (visited on 04/06/2013).

[2] Cynthia Dwork, Andrew Goldberg, and Moni Naor. "On Memory-Bound Functions for Fighting Spam". In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*. Ed. by Dan Boneh. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 426–444. ISBN: 3-540-40674-3. DOI: http://springerlink.metapress.com/openurl.asp?genre=article&issn=0302-9743&volume=2729&spage=426.

[3] Cynthia Dwork and Moni Naor. "Pricing via Processing or Combatting Junk Mail". In: *Advances in Cryptology - CRYPTO 92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*. Ed. by Ernest F. Brickell. Vol. 740. Lecture Notes in Computer Science. Springer, 1992, pp. 139–147. ISBN: 3-540-57340-2. DOI: http://link.springer.de/link/service/series/0558/bibs/0740/07400139.htm.

[4] Ben Laurie and Richard Clayton. *"Proof of Work" proves not to work*. 2004.